# VIRGINIA DEPARTMENT OF EDUCATION

# *SOL Technology Initiative*

## Architectural Guidelines for High School Readiness

Division of Technology
Division of Assessment and Reporting

July 2001

# Table of Contents

# Purpose and Background

## Purpose

This document contains the architectural guidelines for Virginia school divisions that are preparing to participate in the Standards of Learning (SOL) Technology Initiative.

The document contains the following three sections:

- Section 1 contains information on the electronic test delivery system that will be used for online SOL testing.
- Section 2 contains those architectural guidelines that must be implemented in order to meet the goals of the SOL Technology Initiative.
- Section 3 contains "Best Practices" that are strongly recommended for implementation. School divisions may need to adopt one or more of the best practices in order to meet the goals of the initiative.

## Background

The Standards of Learning Technology Initiative is a large-scale project to improve student achievement using technology resources. The 2000 Virginia General Assembly approved the initiative, forwarded by the Governor, that provides funding to schools for the development of an array of web-based instructional and remedial programs, including online delivery of the high school SOL tests.

The initiative, focusing first on Virginia's high schools, includes funding targeted to achieve the following goals:

- Provide a ratio of one computer for every five high school students.
- Create Internet-ready local area network capability in every high school.
- Assure high-speed, high-bandwidth capabilities for instructional, remedial and testing needs in every high school.

NCS Pearson is the vendor selected by the Department of Education to provide an electronic test delivery system for high school SOL testing.

These guidelines are based upon technical and architectural information provided by NCS Pearson. The Virginia Department of Education (VDOE) may update this document periodically throughout the duration of the initiative.

Up-to-date, detailed information about the initiative can be found on the World Wide Web at:

http://www.pen.k12.va.us/VDOE/Technology/soltech/soltech.html.

# 1 The Electronic Test Delivery System

NCS Pearson is a global provider of applications, services, and technologies for education, testing, assessment, and complex data management. The combination of NCS and Pearson Education has created a world leading integrated education company, combining strong market positions in educational content, online learning, assessment, and enterprise applications for U.S. schools and professional accreditation. NCS Pearson is a wholly owned company of Pearson plc, an international media company.

## 1.1 Product Overview

eMeasurement Services, NCS Pearson's (NCS) Web-based test administration system, is Web-based and specifically designed to meet the needs of high-stakes large-scale assessments such as the SOL. NCS used its years of experience in assessment to ensure that the security within eMeasurement Services meets or exceeds what is possible in a paper and pencil testing environment. Access is controlled through a series of user IDs and passwords. All transmissions are encrypted, and no items are left on the local workstation when testing concludes.

The eMeasurement Services' software and SOL test items and data will reside on a central server where NCS maintains both the hardware and the software, ensuring that tests, reports, and data are always available where and when needed.

Reports will be custom designed for Virginia. Similarly, the Department of Education determines who should have access to the various functions within the system. NCS will implement those decisions by assigning user IDs and passwords. There will be a minimal demand on school divisions' IT personnel to maintain, configure, or troubleshoot the testing system. Divisions will be free to use those valuable resources to maintain their own hardware and other services to their schools.

The eMeasurement Service's test delivery module, known as ***TestNav***, is an installed Internet software component that controls test delivery and presentation. The NCS test administration Web page provides the reporting, delivery, and authoring functions of the testing system. Accessing the NCS test administration site requires only a standard Internet browser. More information on ***TestNav*** and a web site for downloading the application will be made available to school divisions at a later date.

# 2 Initiative Requirements

This section provides those recommendations that school divisions are required to implement in order to be ready to meet the goals of the SOL Technology Initiative.

## 2.1 Infrastructure

- Testing locations in each school will need to be evaluated to determine if they have sufficient electrical outlets and network jacks.
- A wireless LAN solution is capable of providing enough bandwidth for current online SOL testing. Special care must be taken to properly segment the wireless portions of the LAN.
- Use only Wired Equivalent Protocol (WEP) compliant wireless LAN solutions. (Almost all new solutions follow this standard.)

  **Note:** Wireless networks may not provide sufficient bandwidth to meet all other instructional needs.

## 2.2 Computer Requirements

All NCS electronic services are delivered via a Web interface. Accessing these services requires access to the Internet and a 4.x or higher version of Netscape or Internet Explorer browsers.

### 2.2.1 Student-to-Computer Ratio

A maximum ratio of five students to one computer must be achieved in each high school. The computers counted for the student-to-computer ratio must meet the minimum requirements defined in the sections below.

### 2.2.2 Client Hardware

The minimum hardware configurations for PC and Macintosh client computers are listed below.

- PC – Pentium 166MHz or better with 32MB RAM, 800x600-video resolution, standard keyboard and pointing device
- Macintosh – PowerPC/PowerMac 200Mhz or better with 32MB RAM or iMac, G3 or better, with 48MB RAM, 800x600-video resolution, standard keyboard and pointing device.

  **Note:** Future versions of ***TestNav*** may require greater hardware requirements. Capabilities for sound, non-standard keyboards and pointing devices may be needed to meet special needs.

### 2.2.3 Client Operating System

The client operating system must be one of the following:

- Windows 95 or higher
- Mac OS 7.6.1 or higher
- Student computers must have their screen savers either shut off or the timeout set to a significantly long time (2 hours). ***TestNav*** will automatically shut down the test if the screen saver activates.
- The control strip on the Macintosh allows access to other applications and some system functions. If the control strip is accessed during a test, ***TestNav*** will automatically shut down. Access to the control strip should be restricted or removed during SOL testing.

  **Note:** Future operating system versions will be evaluated on an ongoing basis.

### 2.2.4 Browsers

The client browser must be one of the following:

- Netscape Navigator 4.0.6 or higher, excluding version 6.x.
- Internet Explorer 4.01 service pack 2 or higher.

### 2.2.5 Test Delivery Module (*TestNav*)

The test delivery module (***TestNav***) is a downloadable Java application. The application is downloaded over the Internet via a secure site in advance of testing.

This test delivery module requires a Java application and Java Virtual Machine (JVM or MRJ on Macintosh) to be installed on each PC delivering a test. As an alternative, the ***TestNav*** and JVM can be installed once on a file server and shared at the desktops by putting a shortcut on each PC delivering a test.

Once installed on a client computer or network, the need for a browser on the client workstation has been eliminated. The downloadable application will also install the Java Virtual Machine on the client system. The versions of the JVM installed by this application are Sun JVM 1.1.8 and Apple MRJ 2.1.4.

**Note:** In a shared installation of ***TestNav***, additional capacity planning will be required to ensure the server has sufficient resources.

**Note:** Write access rights are required to install and update the ***TestNav*** software.

### 2.2.6 Printer Hardware

Generating student test tickets requires a printer. Depending on where and when these are printed, a printer in each testing area may be required.

- A graphics enabled printer is required. Color is not required.

## 2.3 Wide Area Network (WAN) & Bandwidth Chart

- The SOL technology initiative requires each school to have a network connection to the Internet whether it is provided via the division or obtained directly from an Internet Service Provider (ISP).

- When the division shares its Internet connection with more than one school, care must be taken not to over-allocate that Internet connection. The WAN connections are essential to the success of online testing; these connections must be as reliable as possible.

- The Internet connection speed will vary depending on the number of computers in the school and number of students that are testing

concurrently. The *Recommended Internet Bandwidth* chart provides the minimum speeds required for online SOL testing.

**Recommended Internet Bandwidth**

| Number of Concurrent Computers[1] | Bandwidth Required for Testing[2] | Type of Connection[3] |
|---|---|---|
| 20 | 33.3 kbs | 128 kbs |
| 30 | 50 kbs | 128 kbs |
| 60 | 100 kbs | 256 kbs |
| 75 | 125 kbs | 256 kbs |
| 100 | 166 kbs | 512 kbs |
| 150 | 250 kbs | 512 kbs |
| 200 | 333 kbs | T1 (1.5 mbs) |
| 250 | 416 kbs | T1 |
| 900 | 1,500 kbs | T1/T3 break point |

1. **Number of Concurrent Computers**: Represents the number of individual Macintosh or PC computers that could be used concurrently to test students.

2. **Bandwidth**: Represents the MAXIMUM required rate of data transmission, assuming that all students open ***TestNav*** and begin testing simultaneously. Using these guidelines, each test will start within 120 seconds of opening ***TestNav***.

3. **Type of Connection**: Based on the bandwidth requirements in column two and the likelihood of additional LAN/WAN activity occurring during testing, this is the type of Internet connection that is required for a single school.

**Note:** If multiple schools are sharing a single Internet connection and those schools would be testing at the same time, add the individual school requirements to obtain the "total" bandwidth needed for the Internet connection. Typical connection speeds are: T1 (1.5mbs), T3 (44 mbs), OC3 (155 mbs), or OC12 (628 mbs).

**Note**: If other computers will be using the Internet while tests are being conducted, schools will also need to include these when calculating their bandwidth requirements. In other words, plan to increase bandwidth above the numbers listed in the chart.

## 2.4 Security and Internet Filtering

- Effective local security at each division will be critical to the success of the initiative. At a minimum, ALL divisions should have some type of firewall protection between their network and the Internet. One area of particular concern is protection against "denial of service" attacks against a division's Internet connection. It is critical that each division ensure that its firewall solution and ISP protects against this type of attack.

- NCS Pearson will be examining and testing several major Internet URL filtering solutions for use with their eMeasurement solution. When testing is completed, a list of tested packages/solutions will be provided, including any appropriate configuration guidelines, specific model recommendations, etc.

- In addition to standard HTTP traffic, the eMeasurement Services uses Secure Socket Layer (SSL) when communicating between the client computer and the host system. Please be sure the client computers and infrastructure are configured to handle SSL traffic. If your school or division's computer infrastructure uses firewalls or routers with filters, please check to be sure they have been opened for specific traffic over the standard SSL port during SOL testing.

- IP filters must be open to specified IP addresses.

  (NCS Pearson will publish addresses as they become available.)

# 3 Best Practices

While the recommendations in the previous section are required for the SOL Technology Initiative, the Department of Education recognizes that each school location will have a unique technology infrastructure and technical needs. School divisions are not required to adopt all of the best practices found in this section, however, it may be necessary to adopt one or more in order to meet the goals of the Initiative. Adopting the recommendations in this section may also help to ensure that each school division achieves the highest possible return from its information technology infrastructure.

## 3.1 Infrastructure

- All infrastructure projects must comply with appropriate building codes.
- Electrical surge suppression should be installed on all copper cabling (e.g., analog telephone lines, DID and DOD trunk lines) at the demarcation “demark” point inside the building.
- The vendor or cabling contractor should test and certify all components within the cabling plant (e.g., patch cables, patch panels, and wall jacks).
- Thin net cabling (10Base-2) should be replaced with Category 5e or better unshielded twisted pair (UTP).
- New cable installations should use Category 5e UTP or better. Where possible, coaxial backbone cables should be replaced with fiber optic cabling. Priority should be given to those cable runs between buildings. When feasible, install redundant cables and consider routing these cables along a separate path.
- Phone service in the testing location would be needed should it be necessary to contact the NCS help desk during a test administration.
- When using wireless technology, the highest available transmission rate should be used, and the LAN should be segmented as much as possible.
- Wireless LAN implementations should utilize the highest number of WEP keys that are possible and / or practical and ensure the keys used are changed from their default values.
- Virtual Private Network (VPN) software is used to ensure proper authentication of wireless devices / users.

## 3.2 Computers

- Desktops and workstations should be plugged into an electrical surge suppression device.

- Essential software applications and device drivers (e.g., virus scanners, network card software, and operating system patches) should be kept up-to-date.

- Schools may determine it is necessary to manually verify every desktop is configured properly. In such cases, it is advisable to review other procedures pertaining to the desktops (e.g., asset tracking, desktop security, and software inventory) before starting the configuration process, since additional requirements may be uncovered.

## 3.3 Wide Area Network (WAN)

- Network servers and other software applications should not be used to route traffic. Use routers, switches, or enhanced firewalls to segment and route network traffic.

- To help alleviate bandwidth constraints, consider installing Web-caching devices. This can have significant improvements on other Web-based activity where students are accessing “static” content or standard HTML pages.

  **Note:** This will not help with the testing requirements because test content cannot be cached.

## 3.4 Local Area Network (LAN)

- Unneeded protocols and services should be removed from workstations and servers. Standardize on Transmission Control Protocol/Internet Protocol (TCP/IP) as the network protocol.

- Names for each device on the network should follow geographical boundaries or function. Define a scheme for naming and assigning addresses to each device on the network. Use private (i.e., not assigned to anyone on the Internet) IP addresses.

- Local DNS (Domain Name Service) services at the school and district level will improve name resolution and manageability. Consider using DHCP (dynamically assigned IP addresses).

- Token Ring should be removed. Migrate to an Ethernet topology.
- Shared hubs should be replaced with 10/100 Ethernet switches.
- A mechanism for managing the network and capturing performance statistics should be created and implemented.
- A diagram of the network infrastructure should be developed using a copy of the building blueprints and kept up-to-date.

### 3.5 Network Equipment/Servers

- Critical applications and servers should be identified and backed up regularly. Regularly verify the backups are working correctly by restoring a test file or test server.
- File servers should be plugged into an uninterruptible power supply (UPS). Schools may also use a UPS for voice systems. Minimally, thirty minutes of battery backup should be provided for these systems. Preferably, in a power outage, the UPS would automatically shut down the servers in a controlled manner.
- All network equipment (e.g., routers and switches) should be plugged into a UPS. Fifteen minutes of battery backup is generally sufficient.
- All network equipment and servers should be plugged into an electrical surge suppression device.
- Servers and networking components (e.g., switches, routers) should be housed in secured, climate-controlled areas. Use racks or cabinets to alleviate space constraints. Your cable or hardware vendor may offer these products.
- Wiring closets should not be shared with janitorial supplies. Corrosive chemicals, equipment (i.e., mop handles) and humidity can cause significant damage.
- Adequate space should be provided for a technician to gain easy access to the front and rear of network equipment and servers.
- Essential software applications and device drivers (e.g., virus scanners, network card software, and operating system patches) should be kept up-to-date.

## 3.6 Procurement

- Widely available computing platforms with the most powerful components should be purchased to increase the useful lifetime of the devices.

- Network hardware and workstations should be procured from major providers or their designated representatives. These providers use commercial grade components with lower failure rates but, more importantly, provide greater consistency in product offerings. Over time, a consistent product base will reduce administration and support significantly.

- Extended (1-3 years) on-site warranty options should be considered when selecting vendor(s).